

ARUBA CENTRAL SWITCHING QUICK START

Contents

Revision History	3
Purpose	4
Start Here	4
Prerequisites	4
Aruba CX switch platforms.....	4
Supported hardware and software	4
Connectivity requirements	4
VSF stacking (6200 and 6300 series)	5
Password requirements for templates	5
Miscellaneous operating notes	6
AOS-Switch platforms	6
Supported hardware and software	6
Connectivity requirements	6
Central account sign-up	7
Onboarding workflow	8
Adding switches to inventory	8
License assignment	8
Group management	9
Aruba switch configuration	11
AOS-CX UI configuration	11
MultiEdit	12
Configuration editing.....	12
Express Config.....	13
AOS-Switch UI configuration	14
Template creation and application	14
Troubleshooting switch connectivity to Central.....	17
Applicable platforms	19

Revision History

Document Version	Reason for Change	Revision Date
1.0 (Initial Release)		Jul 2021

Purpose

Aruba Central can be used to streamline deployment of switches, gateway controllers, and wireless access points. This guide can be used to quickly set up a new Central account, onboard devices, and manage switches based on the AOS-CX and AOS-Switch platforms.

Start Here

In addition to this Quick Start guide, a [video series](#) is available on YouTube, and additional resources are available in the **Resources** section at the end of this document.

Prerequisites

Aruba CX switch platforms

Supported hardware and software

The listed Aruba CX switch models running the minimum listed software versions are supported in Aruba Central.

Any switch model running an older version than the minimum supported must be updated prior to being onboarded.

The *recommended* software release for switches being managed by Central is **10.06.0110** or later. Switch software downloads can be found on the [Aruba Support Portal](#), or via Central's firmware update functionality.

Platform	Minimum Version	Recommended Version	Config Group Types
6100	10.06.0110	10.06.0110	Template
6200	10.05.0021	10.06.0101	UI and Template
6300	10.05.0021	10.06.0101	UI and Template
6300 (JL762A)	10.06.0001	10.06.0101	UI and Template
6405	10.05.0021	10.06.0101	Template
6410	10.05.0021	10.06.0101	Template
8320	10.05.0021	10.06.0101	UI and Template
8325	10.05.0021	10.06.0101	UI and Template
8360	10.06.0001	10.06.0101	UI and Template
8400	10.06.0001	10.06.0101	Template

Connectivity requirements

In order to be managed by Central, Aruba CX switches require an Internet connection on either the **default** VRF or **mgmt** VRF; this may be a direct ISP connection, through a NAT router and/or firewall, or via HTTP proxy. A DNS service capable of resolving the public hostnames of the Activate and Central services must be accessible from the switch. If there is a firewall between the switch and Central, permit outbound connections using TCP port 443 (SSL/TLS) to the appropriate Activate and Central URLs listed [here](#).

To connect to Central via HTTP proxy server, the switch must be running AOS-CX 10.7 or later; the proxy FQDN or IPv4 address may be configured from the switch CLI or using DHCP vendor-specific suboption 148. The HTTP proxy configuration uses one of the following string formats:

- Fully-qualified domain name (FQDN): `http-proxy.arubanetworks.com:8088`
- IPv4 address: `192.168.1.254:8088`

Note: HTTPS and SOCKS proxy servers are not supported.

Use the `http-proxy` CLI command from the switch **config** context to manually configure the proxy server:

```
switch(config)# http-proxy 192.168.1.254:8088 vrf mgmt
```

If the proxy setting is received via DHCP option, the VRF on which the DHCP option was received is used automatically. When the HTTP proxy is manually configured via the CLI, a specific VRF (such as the **mgmt** VRF) can be specified to use the proxy connection; if none is specified, the **default** VRF is used. A manually-configured HTTP proxy will override any proxy settings received from other sources.

For AOS-CX software upgrades, a minimum of 2 Mbps of Internet downlink bandwidth is required for each switch being upgraded in parallel; image transfers must be completed within a 60-minute software upgrade timeout period.

VSF stacking (6200 and 6300 series)

Central is capable of managing 6200 and 6300 VSF stacks in both UI and template groups. If a stack will be managed as a member of a UI group, it must be fully provisioned prior to being onboarded. Stacks to be managed in template groups may be provisioned using the VSF auto-stacking feature and the downloaded configuration template.

Note: To use auto-stacking to provision a VSF stack with a Central configuration template, all stack members must be in a factory default state running AOS-CX 10.7 or later, with VSF links connected to match the VSF template configuration.

The following tasks for template-managed VSF stacks require disabling Central management, making the necessary changes locally, then modifying the template to reflect the updated stack configuration before re-enabling Central management:

- Adding or removing members
- Replacing stack members with a different model
- Changing the standby member ID
- Modifying, adding, or removing VSF links

Central configuration templates will only be synced to VSF stacks where the stack primary (member ID 1) is operating as the stack Conductor; if a failover has occurred and the secondary is operating as the conductor, configuration syncing will not occur. The stack must be returned to normal operation with the stack primary operating as conductor to resume Central template configuration syncing.

Password requirements for templates

For Aruba CX switches being managed by configuration templates, Central requires the switch admin password (or the password of at least one other user belonging to the switch *administrators* user group) to be specified in plaintext, either hardcoded into the template itself or substituted as a variable. For this reason, it is important to restrict access to Central management functions to only authorized administrators. (Note that the switch management connection to Central is encrypted via TLS, preventing interception of these credentials in transit.)

When an Aruba CX configuration is imported into Central as a template, any passwords defined in the configuration are imported as ciphertext; before the template can be saved and applied to switches in the group, at least one password for a user in the *administrators* group must be changed to the equivalent plaintext or replaced with a variable containing the plaintext password.

A factory default switch, assigned to a template group before provisioning, will use passwords defined in the downloaded configuration template upon initial connection to Central.

In the event of a mismatch between admin user passwords between a switch and the applicable Central template, or if there is no applicable configuration template in the group, no configuration will be pushed and Central will be limited to basic monitoring functionality until an applicable template with a matching admin user password is present.

Miscellaneous operating notes

The following additional notes apply to Central-managed Aruba CX switches:

- All in-band switch ports on 8320, 8325, 8360, and 8400 switches are disabled by default; to manage these switches using in-band ports, pre-configuration from the switch console or Aruba CX mobile app is required to enable at least one in-band port, assign IP addressing and DNS server settings, and enable SSH and HTTPS server processes on the default VRF
- Usage of the `vsx-sync` feature is not recommended for VSX pairs (6400, 8320, 8325, 8360, 8400) being managed by a common template
 - Use of variables and conditional checks to distinguish between VSX primary and secondary roles is strongly recommended for VSX pairs being managed within a single template group
- To use the remote console feature, the SSH server process must be enabled on the VRF being used by the switch to connect to Central
- To restore a switch to factory default settings before onboarding it to Central, use the `erase all zeroize` command instead of `erase startup-config`

AOS-Switch platforms

Supported hardware and software

The following AOS-Switch hardware platforms and software versions are supported by Aruba Central for device management, with the specified configuration group types supported for each platform.

Platform	Minimum Version	Recommended Version	Config Group Types
2530	YA/YB.16.05.0008	YA/YB.16.10.0015	UI and Template
2540	YC.16.03.0004	YC.16.10.0015	UI and Template
2920	WB.16.03.0004	WB.16.10.0015	UI and Template
2930F	WC.16.03.0004	WC.16.10.0015	UI and Template
2930M	WC.16.04.0008	WC.16.10.0015	UI and Template
3810M	KB.16.03.0004	KB.16.10.0015	UI and Template
5400R	KB.16.04.0008	KB.16.10.0015	Template

Connectivity requirements

AOS-Switch devices require either a direct Internet connection or connection via a proxy server, as with Aruba CX switch platforms. AOS-Switch uses the same protocols and web endpoints for Activate and Central as AOS-CX, and the requirement to allow outbound TLS connections to Activate and Central FQDNs on TCP port 443 applies.

The HTTP proxy FQDN or IPv4 address and TCP port may be configured via DHCP vendor-specific suboption 148 or via the CLI, using one of the following string formats:

- Fully-qualified domain name (FQDN): `http://http-proxy.arubanetworks.com:8088`
- IPv4 address: `http://192.168.1.254:8088`

Note: HTTPS and SOCKS proxy servers are not supported.

Use the `proxy server` command from the CLI config context to configure the HTTP proxy server:

```
switch(config)# proxy server http://http-proxy.arubanetworks.com:8088
```

To add an exception to the switch proxy settings for a hostname, IPv4 address, or IPv4 subnet, use the `proxy exception` CLI command from the config context:

```
switch(config)# proxy exception ip 192.168.1.0/24
```

The switch will bypass the configured proxy server for connections to services using hostnames or IPv4 addresses/subnets configured as exceptions.

Central account sign-up

The first step is to ensure you have a working Aruba Central account. If you do not already have an account, open [this sign-up page](#) and enter the requested information. Select the appropriate regional server cluster from the **Server Details** dropdown list, and choose which applications you wish to evaluate — **Network Operations** is the application used for device management and monitoring, so ensure that its box is checked. Once the form has been completed and you have reviewed and agreed to the Terms and Conditions, select **Sign Up**.

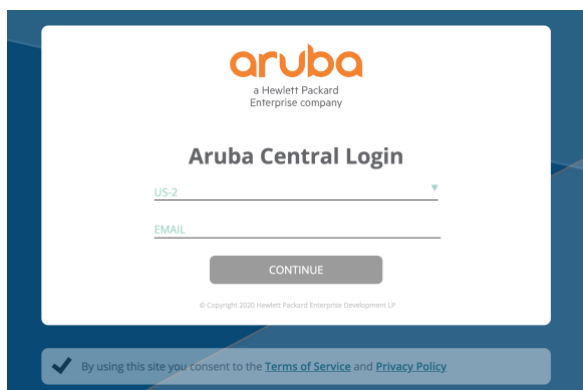
When you are prompted to verify your email address, check your inbox for the verification email and use the link in the email to complete the verification process.

ONE LAST STEP.

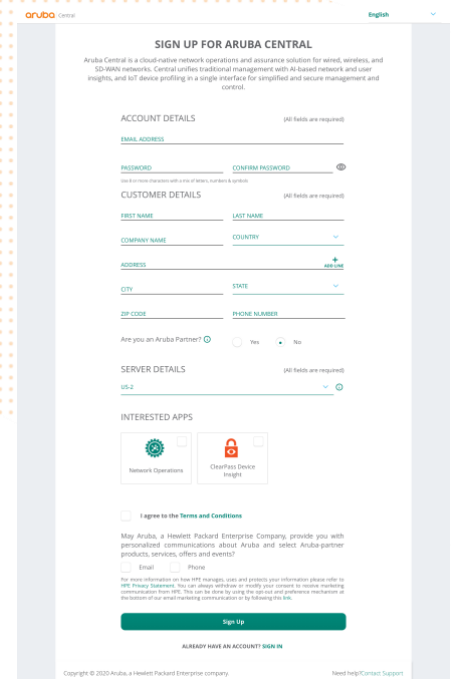
We have sent you an e-mail to validate your account.
Please click the link in the e-mail to register and start using our services.

[Resend Verification Email](#)

Once the signup process is complete, open the [Central portal](#) page, select the server cluster you specified during signup, and use your credentials to sign in.



The image shows the Aruba Central Login page. At the top, the Aruba logo is displayed with the text "a Hewlett Packard Enterprise company". Below the logo, the heading "Aruba Central Login" is centered. There are two input fields: "US-2" with a dropdown arrow and "EMAIL". Below these fields is a "CONTINUE" button. At the bottom, there is a checkbox with the text "By using this site you consent to the Terms of Service and Privacy Policy".



The image shows the "SIGN UP FOR ARUBA CENTRAL" page. It includes a header with the Aruba Central logo and a language selector set to "English". The main heading is "SIGN UP FOR ARUBA CENTRAL". Below this, a sub-header states: "Aruba Central is a cloud-native network operations and assurance solution for wired, wireless, and SD-WAN networks. Central unifies traditional management with AI-based network and user insights, and IoT device profiling in a single interface for simplified and secure management and control." The form is divided into several sections: "ACCOUNT DETAILS" (Email Address, Password, Confirm Password), "CUSTOMER DETAILS" (First Name, Last Name, Company Name, Country, Address, City, State, ZIP Code, Phone Number), "SERVER DETAILS" (US-2), and "INTERESTED APPS" (Network Operations, ClearPass Device Insight). There is a checkbox for "I agree to the Terms and Conditions" and a "Sign Up" button at the bottom. A footer contains copyright information and a link to "Need help? Contact Support".

Onboarding workflow

Adding switches to inventory

After logging into Central for the first time, you will be presented with a "Welcome to Aruba Central" page. Choose the **EVALUATE NOW** link to continue to the onboarding workflow, or if you have paid subscription keys, instead choose **GET STARTED**.

The onboarding workflow will prompt you to add at least one device to Central. Select **ADD DEVICE**, then enter the serial number and MAC address for each switch. If you would prefer to add devices via Activate or CSV import, instead select **EXIT WORKFLOW**.

Note: Activate sync and CSV bulk import require at least one paid subscription key to be assigned to the Central account.

Each device is validated as its entry is completed, and will be added automatically with a "Device added successfully" status message displayed below the serial number. If the serial number and MAC address do not match, or if a device that is already being managed by another Central account is entered, a red error message such as "Blocked device" will be displayed instead.

To onboard a large number of devices, exit the onboarding workflow using the **EXIT WORKFLOW** link.

Open the Account Home page using the highlighted icon in the top-right corner, then open the **DEVICE**

INVENTORY page. Use either the **Sync Devices** button to import devices from an associated Activate account, or **Import Via CSV** to use a locally-generated device list. See the **Appendix** for a CSV example.

When finished adding devices, click or tap **DONE**, then **ASSIGN GROUPS**.

License assignment

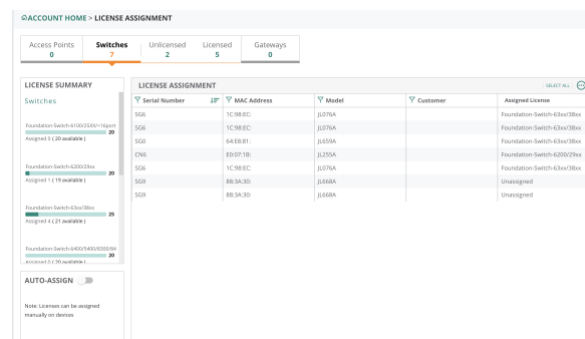
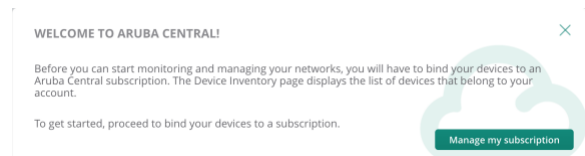
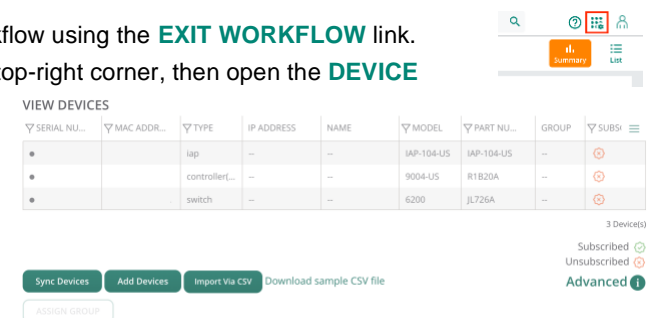
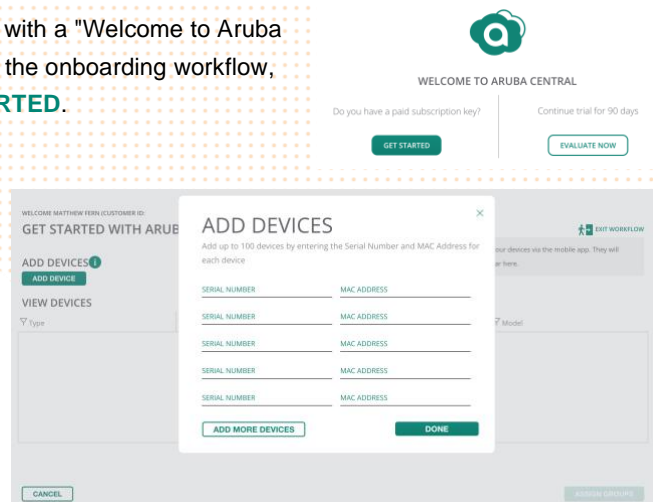
Before actually assigning switches to groups, they must first be assigned device management licenses. When prompted, select **Manage my subscription** from the pop-up, or return to the account home page and select **LICENSE ASSIGNMENT**.

The current release of Central uses a licensing model based on device families and feature levels. Switch licenses are divided into the following four groups:

- 2530, 2540, 6100, all other switch models ≤ 16 ports
- 2920, 2930, 6200
- 3810, 6300
- 5400R, 6400, 8320, 8325, 8360, 8400

There are two feature levels of licenses currently defined in Central for switch management: **Foundation** and **Advanced**. Currently, all switch management functionality is provided by the **Foundation** license type.

There are two methods of assigning device management licenses. The first is to use the **auto-assign** feature; when enabled, all devices added to the Central account inventory will automatically be assigned licenses until the available license pool for that device family is exhausted.



The second method is to manually assign device subscriptions. To assign a subscription to one or more devices, highlight them by selecting each entry in the list, then choose **MANAGE ASSIGNMENT**. Choose the **FOUNDATION** license type, and select **Update**.

To unassign licenses from devices, highlight them in the list, select **MANAGE ASSIGNMENT**, then select **Unassign**.

MANAGE LICENSE ASSIGNMENT (MANUAL)

Overview of selected Switches

Unassigned	2
------------	---

Choose License Type

FOUNDATION

Cancel

Unassign

Update

Group management

Return to the account home page and launch **Network Operations**.

ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

APPS

Unassigned: 0 (0% left)



Network Operations
Manage your wired, wireless, and WAN infrastructure

LAUNCH

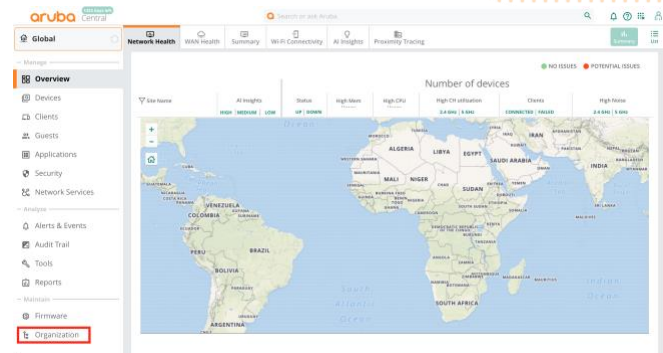
Unassigned: 0 (0% left)



ClearPass Device Insight
Discover and Profile devices connected to the network

LAUNCH

Navigate to the **Organization** page using the navigation menu on the left side of the window.



This opens the Groups listing. This page lists groups that have been created for this Central account, and devices that have been assigned to each of them. Any devices that are online but have not yet been assigned to a group are listed under **UNASSIGNED DEVICES**.

To create a new group to manage onboarded switches, select **New Group** from under the group listing on the left side of the page.

The screenshot shows the 'Groups' management page in Aruba Central. The left sidebar has 'Groups' selected. The main content area is titled 'GROUPS' and includes a description: 'A group in Aruba Central acts like a primary configuration container for devices. You can combine devices with common configuration requirements into a single group and apply the same configuration settings to all the devices in the group.' Below this is a 'MANAGE GROUPS' section with instructions: 'DRAG AND DROP CLUSTERS AND SWITCHES BETWEEN GROUPS' and 'TO SELECT MULTIPLE DEVICES SHIFT-CLICK OR CTRL-CLICK'. There are two tables. The first table, 'Group Name' vs 'Devices', shows 'ALL CONNECTED DE...' with 1 device, 'UNASSIGNED DEVI...' with 1 device, 'TG: 6300-standalone' with 0 devices, 'TG: 6300-VSF-2mem' with 0 devices, and 'default' with 0 devices. The second table, 'Name' vs 'Location' vs 'Type' vs 'Serial #' vs 'MAC Address', shows a single entry for '6300-1' with location 'Aruba CX'. At the bottom, there are buttons for 'New Group', 'Import Configuration to New Group', and '1 Device(s)'.

Give the new group a name. To create a UI configuration group for switches, leave the **SWITCH** checkbox unchecked; to instead create a template configuration group, check the box. The **IAP AND GATEWAY** checkbox only applies to those device types, and has no effect on switch configuration regardless of its setting.

If either the **IAP AND GATEWAY** or **SWITCH** checkboxes are unchecked to use UI configuration, enter an admin user password under the **Group password settings** prompt; this password will be used for admin user authentication for all devices assigned to this group. Select **Add Group** to finish group creation.

Once the group has been created, select either **ALL CONNECTED DEVICES**, **UNASSIGNED DEVICES**, or **default** from the group list. Select one or more switches to be assigned to the newly created group, then drag them over to the group that was just created. If the switch you wish to move into the group is not visible, ensure it is connected to the Internet and running the minimum supported version, and try again.

When prompted to confirm the move, review the alert in the popup. Note that if you are moving switches into a group with no existing or applicable templates, no configuration changes will occur. However, if the destination group has at least one template that applies to any switches assigned to it, their existing configuration will be replaced with the template configuration.

Note: Before moving a VSF stack into a template group, first ensure that any template that could be applicable to that stack contains the proper VSF member and link configuration to avoid disruption of stack operations.

Select **Yes** to confirm the move.

Once switches have been moved into the group, select the gear icon next to the group name to open the group configuration page.

To assign switches to a group before they have been connected to Central for the first time, return to Account Home and open the **DEVICE INVENTORY** page. Highlight one or more switches from the device list, and select **ASSIGN GROUP**. Choose the desired group, then select **Assign Device(s)**. When these switches connect to Central, they will be attached to the explicitly assigned group instead of the **default** group.

CREATE NEW GROUP

GROUP NAME
Switch UI Config

Use the group as Template group by selecting the device

☐ IAP AND GATEWAY ☐ SWITCH

Group password settings

PASSWORD

CONFIRM PASSWORD

Cancel Add Group

MANAGE GROUPS

DRAG AND DROP CLUSTERS AND SWITCHES BETWEEN GROUPS
TO SELECT MULTIPLE DEVICES SHIFT+CLICK OR CTRL+CLICK

Group Name	Devices	Group Name	Location	Type	Serial #	MAC Address
ALL CONNECTED DE...	1	6300-1		Aruba CX		
UNASSIGNED DEVIC...	1					
CX-TemplateGro...	0	6300-1		Aruba CX		
default	0					

CONFIRM ACTION

Moving 1 device(s) from unprovisioned to CX-Tem plateGroup. Moving devices to another group changes the configuration of the selected devices. Device Level configuration for STACKED SWITCHES have to be reconfigur ed. Do you want to continue?

Yes No

Group Name	Devices
ALL CONNECTED DE...	1
UNASSIGNED DEVIC...	0
CX-TemplateGro...	1
default	0

DEVICES

Seri...	IF	MA...	Par...	Mo...
SG9	88-3A-3D	JL668A	6300	
SG9	88-3A-3D	JL668A	6300	
SG6	1C-98-EC	JL076A	3810	
SG6	1C-98-EC	JL076A	3810	
SG6	1C-98-EC	JL076A	3810	
SG0	64-EB-B1	JL659A	6300	
CN6	E0-07-1B	JL255A	2930F	

ASSIGN GROUP

GROUP NAME

3810-Stack

6300-TG

CX-Demo

default

Template Holding

5 Group(s)

Cancel Assign Device(s)

Aruba switch configuration

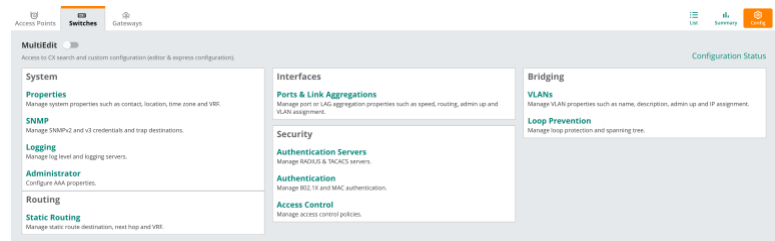
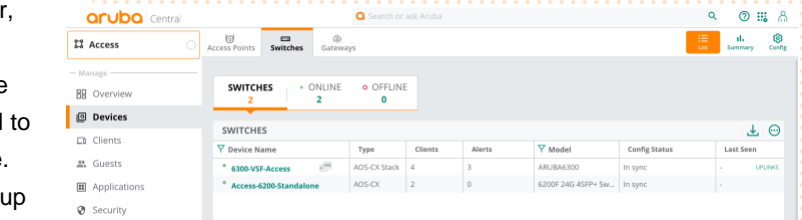
AOS-CX UI configuration

Note: Moving a configured Aruba CX switch into a UI configuration group will immediately replace the switch configuration with the group configuration. Migration from template configuration groups to UI configuration groups is not currently supported for Aruba CX switches.

From the group context, displayed in the top left corner, open the **Devices** page from the left hand navigation menu, then select the **Switches** tab from the bar at the top. This displays the list of switches that are assigned to the group and have connected to Central at least once. Select the **Config** link in the top-right corner; if the group contains no devices, or a mix of AOS-Switch and AOS-CX switches, instead select the **AOS-CX** link.

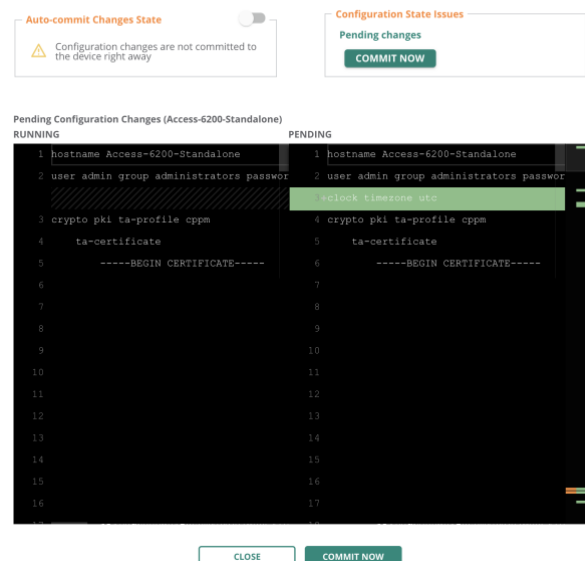
Feature-level configuration is divided into five distinct categories:


- **System:** Basic system properties, SNMP, logging, and management access controls
- **Routing:** Static route definitions
- **Interfaces:** Port and link aggregation group (LAG) settings, VLAN assignments
- **Security:** Port access and ACL settings
- **Bridging:** VLAN definitions, loop protection, and spanning tree

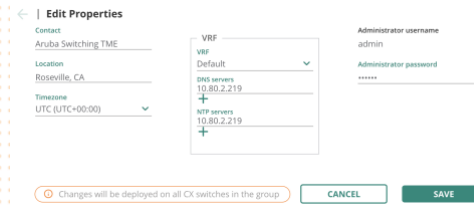


Configuration changes can be made at the **group** context or **individual switch** context, with the current context displayed in the top-left corner. Certain settings, such as interface IP addressing, can only be changed at the individual switch context. For settings that exist at both the group and individual device contexts, the *most recent change* prevails — a setting changed at the device level will be overridden by a later change to the same setting made at the group level, and vice versa.

By default, any configuration changes made in the Central UI are applied immediately to all managed switches in the group. This setting, auto-commit, can be changed at the individual switch level. To do so, return to the group device list using the **List** icon in the top-right corner. Select the desired switch using the link in the Device Name column. Open the Device page from the left-hand navigation menu, then select Configuration Status in the top-right corner of the page. The auto-commit setting can be enabled or disabled using the toggle button on the left side of the page. When auto-commit is disabled, pending configuration changes can be reviewed from the Configuration Status page before being committed to the switch configuration.



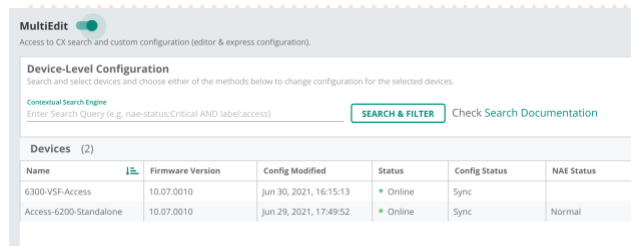
To modify settings, select the appropriate link under each heading. To return to the main configuration page without making changes, select the  icon in the top-left corner. Once changes have been made and validated, select the **SAVE** button to apply them and return to the main configuration UI. To discard the changes and return to the main configuration page, instead select **CANCEL**.



Note: To prevent interruption of the Central management connection if switches in the group will be assigned static IP addresses, first ensure that the appropriate static routes are defined on the **Static Routing** page or use MultiEdit mode to define any necessary routing protocols before changing the IP address from the device-level context.

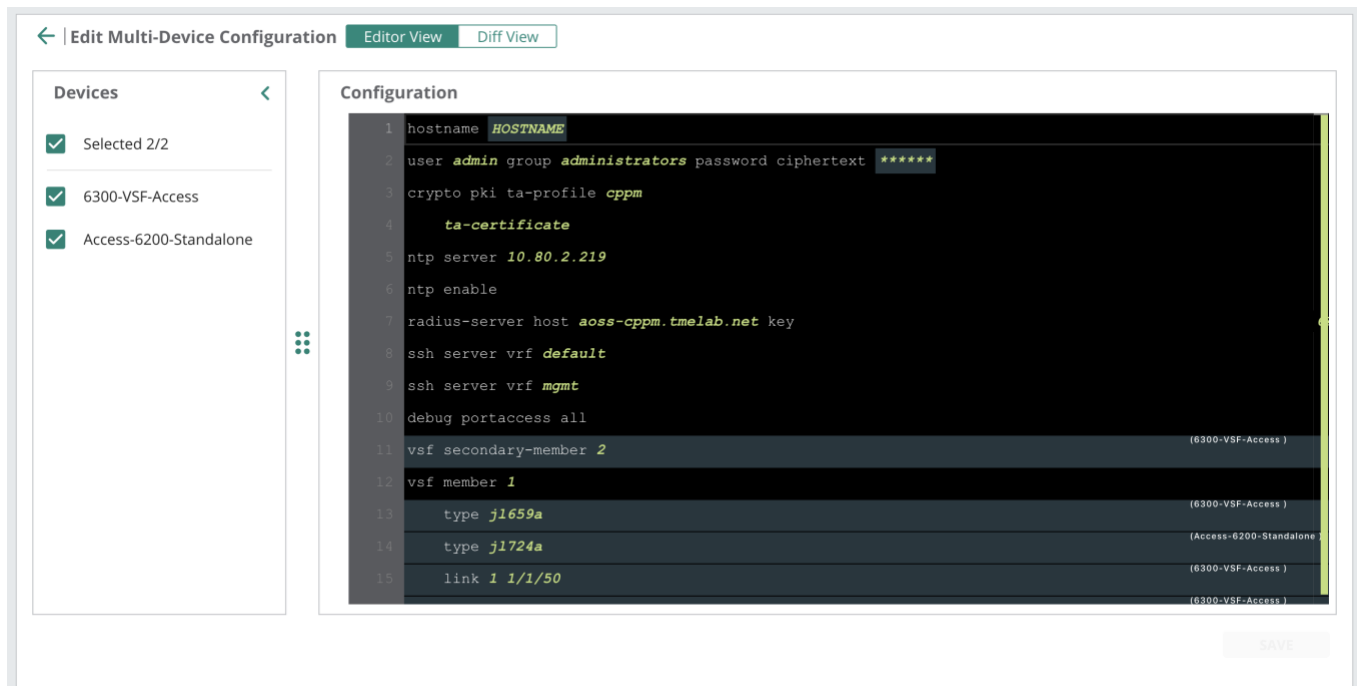
MultiEdit

Enable MultiEdit mode by selecting the toggle switch on the top of the group Config page. This will open a device list from which one or more devices can be selected to view or modify the switch configuration, or utilize the Express Config feature to deploy Network Analytics Engine agents or device profile settings.




Configuration editing

Highlight at least one device in the list, and select **EDIT CONFIG** from the pop-up in the bottom right corner. This opens the configuration editor UI for the selected switches.



Note: The MultiEdit configuration editor UI uses the indentation level of the cursor to determine the current command context, with the furthest left column being equivalent to the top-level **config** context in the AOS-CX CLI, adding indentation in increments of 4 spaces per feature-specific context level.

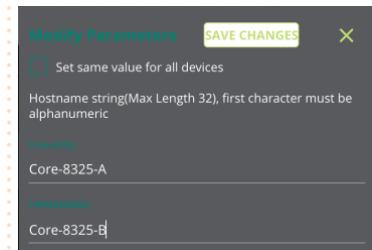
To hide or show device configurations from the editor view, uncheck or check each device from the list on the left; use the  icon to minimize the device list and maximize the editor view.

When multiple switch configurations are displayed simultaneously, the following notes apply:

- **Any** portion of the configuration that differs between the switches currently displayed is highlighted in green
- If a specific configuration line only exists on a subset of the displayed switches, the name of the applicable switch is

- displayed near the top-right corner of that line
- For most commands that exist on all currently displayed switches, only the specific parameters that differ are highlighted and displayed as a placeholder, such as the **hostname** in the example above

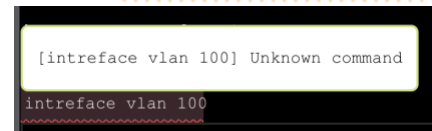
To modify any command or parameter that exists, but is different, for multiple displayed devices, right-click the highlighted placeholder to open the **Modify Parameters** pop-up; after making changes, select **SAVE CHANGES** from inside the pop-up (*not* the **SAVE** button in the bottom-right corner) to return to the editor.



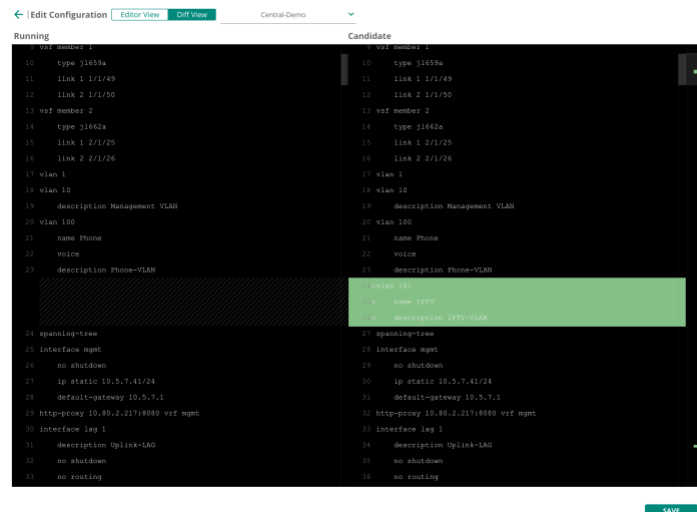
The configuration editor provides autocompletion and syntax validation functionality. The autocomplete feature displays valid commands and parameters below the line being edited based on characters that have already been entered, and can be utilized by selecting the desired command or parameter from the displayed list using the up/down arrow and Tab keys or by using the mouse pointer or touch screen.



Syntax validation ensures that only valid commands are entered; syntax errors are denoted by highlighting and underlining the applicable line in red, and the detected error is displayed by hovering the mouse pointer over the highlighted portion of the line. Common syntax errors include typographical errors, invalid parameters, or entering commands or parameters outside of a supported context (see note above).

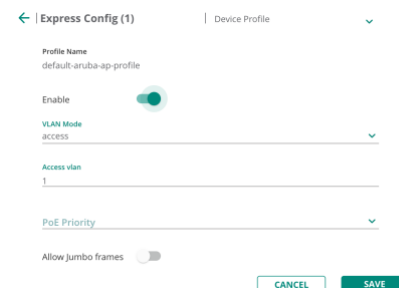


When finished making changes, use the **Diff View** to compare the current running configuration with the edited candidate configuration; changes are highlighted in green and/or orange. Select **SAVE** to apply the candidate configuration to the selected devices.



Express Config

The Express Config workflow can be used to deploy Aruba AP device profile settings or selected Network Analytics Engine agents to a managed Aruba CX switch. Select one or more switches from the device list, and choose **EXPRESS CONFIG**. Select either Device Profile or Network Analytics Engine from the drop-down menu in the top-right, and choose an agent from the **NAE Script Name** menu (if applicable). Modify settings for the selected feature or NAE agent as desired, then select **SAVE** to deploy the profile or agent to the selected switches.

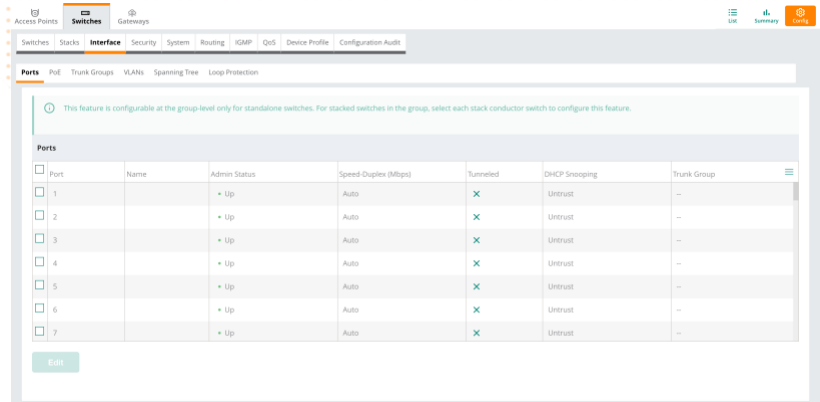


AOS-Switch UI configuration

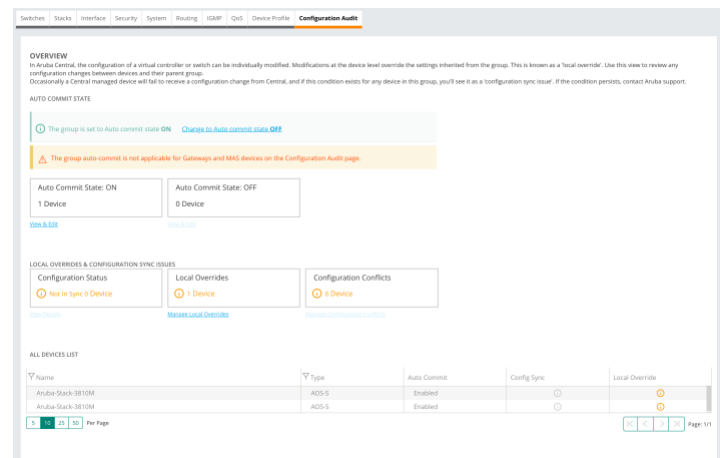
Note: Moving a configured AOS-Switch device into a UI configuration group will result in the switch configuration being immediately replaced with the group configuration, unless auto-commit has been disabled at the group level.

Feature-level configuration is grouped under the following tab-based headings:

- **Switches:** Basic system properties
- **Stacks:** Virtual Switching Framework (VSF) and backplane stacking (BPS) deployment and configuration
- **Interface:** Port, PoE, trunk group (LAG), VLAN, spanning tree, and loop protection
- **Security:** Access policies, DHCP snooping, rate limiting, RADIUS, downloadable user roles, authentication, and tunneling
- **System:** Management access, DNS, time synchronization, SNMP, Cisco Discovery Protocol (CDP), DHCP
- **Routing:** IP routing setting, Static route definitions
- **IGMP:** VLAN-level IGMP configuration, unknown multicast filtering
- **QoS:** QoS traffic policy definitions and DSCP mapping
- **Device Profile:** Aruba AP profile settings



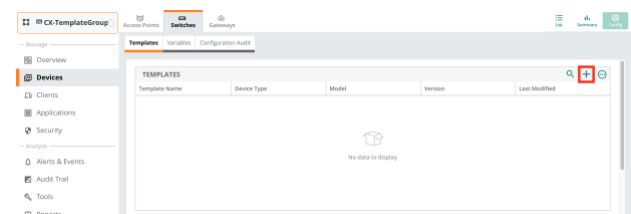
To modify settings, choose the appropriate section from the tab bar across the top of the group configuration UI, as well as the desired subsection where required. Once changes have been made and reviewed, select **SAVE** from the feature settings pop-up; changes will be applied immediately unless auto-commit has been disabled at the device or group level, in which case they would be manually committed to devices by the administrator from the **Configuration Audit** page.



Template creation and application

From the group's **Devices** page, open the **Switches** tab from the top navigation bar, then **Config** in the top-right corner.

This opens the group template management page. In a newly-created group, this list will be empty. Select the **+** icon in the top-right corner of the template list to create a new template.



The template name, like group names, cannot contain spaces. Select the appropriate device type: **Aruba Switch** (AOS-Switch) or **Aruba CX**. You may either choose specific device models, part names, and software versions to which the new template will apply, or select **ALL** for one or more of these to create a more generic template that may apply to a range of switches. Select **NEXT** to continue.

This opens the template editor. If this is the first template being created for the current group, it must be entered manually (see the appendix for generic template examples that can be copied and pasted into the editor, or use an existing switch configuration as a baseline).

While there is an option to import the configuration from an existing switch as a new template, this may only be used if Central has already successfully authenticated against the switch — for instance, if the switch was already being managed by the current Central account as part of another group.

Templates may contain *variables* and *conditional statements* (if, else) in order to apply the same template to multiple devices without also applying the same values (such as IP addresses or hostnames) to those devices. These functions are utilized by enclosing the variable or conditional statement in ‘%’ characters, as in the following examples:

```
hostname %_sys_hostname%
%if vlan_1_dhcp%
ip dhcp
%else%
ip address %vlan_1_ip%
no ip dhcp
%endif%
```

Note: An `%endif%` statement must be present for every `%if%` statement present in the template; any mismatch between the number of `%if%` and `%endif%` statements will be flagged as a template syntax error and the affected template will not be applied to any managed devices until the error is corrected.

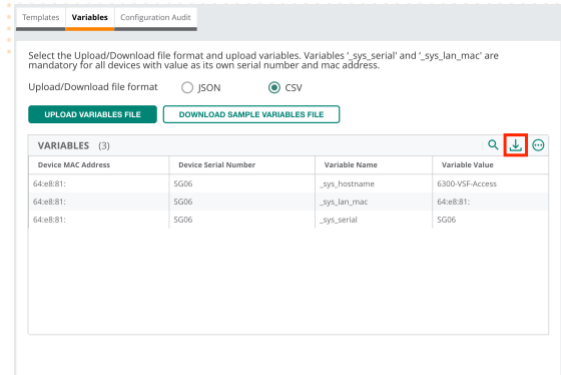
Variables and conditional statements can be used to define a template that selectively applies portions of a template based on the specific value contained in the variable; in the following example, the `Stack_Members_Total` variable is used to define the size of a particular VSF stack; the `=` and `>=` comparisons are used to check the value contained in the variable to determine which portion of the template is actually applied:

```
vsf member 1
type %Stack_Member_1_Model%
%if Stack_Members_Total>=2%
link 1 %Stack_Member_1_Link_1_Interface%
link 2 %Stack_Member_1_Link_2_Interface%
vsf secondary-member 2
vsf member 2
type %Stack_Member_2_Model%
link 1 %Stack_Member_2_Link_1_Interface%
link 2 %Stack_Member_2_Link_2_Interface%
%endif%
```

```
%if Stack_Members_Total>=3%
    vsf member 3
    type %Stack_Member_3_Model%
    link 1 %Stack_Member_3_Link_1_Interface%
    link 2 %Stack_Member_3_Link_2_Interface%
%endif%
%if Stack_Members_Total>=4%
    vsf member 4
    type %Stack_Member_4_Model%
    link 1 %Stack_Member_4_Link_1_Interface%
    link 2 %Stack_Member_4_Link_2_Interface%
%endif%
```

If the value for `Stack_Members_Total` is *less than* the value being checked, that portion of the template up to the following `%endif%` statement is skipped; if the variable is not defined at all or does not contain any value (i.e. the value is an empty string), *any* section bounded by a non-empty conditional check for that variable will be skipped.

Variables are defined on a per-device or per-stack basis, and may be edited either within Central itself or offline using a downloaded copy of the variable set for the displayed group or device. Select the desired upload/download file format (JSON or CSV), then use the highlighted download button in the top-right corner of the variable list to download the group variable file. Make any desired changes, then re-upload the modified file using the **UPLOAD VARIABLES FILE** button.



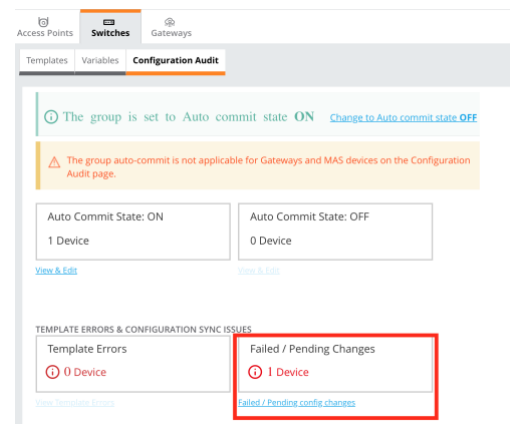
Note: The CSV variable file format contains a Modified field for each device in the file, with a default value of N; change this value to Y for any device with modified variables that will need to be updated when the file is uploaded.

Once the new template has been created, select **SAVE**. The template will immediately be applied to all specified devices in the group, so ensure that it has been reviewed for possible effects on connectivity and features prior to saving it.

Note that when multiple templates are present that may apply to a given switch assigned to the group, Central automatically selects the *most specific* template — the template that matches the most parameters (model, part name, and version) — to apply to that switch.

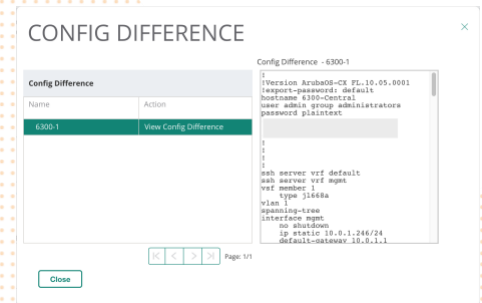
Once the template has been saved, open the **Configuration Audit** page. The first thing you might notice is that the **Failed / Pending Changes** portion of the page lists 1 or more devices. This is usually normal; it indicates that a configuration change (either to the template or variables) has been detected and a configuration change has been queued to be pushed to affected devices.

Select the **Failed / Pending config changes** link below the box.

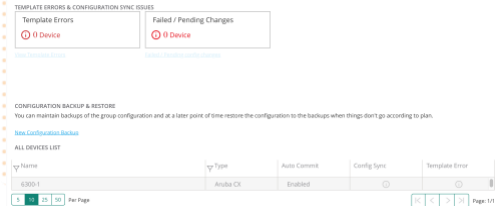


Choose a displayed device in the list and select **View Config Difference**. If the template has no syntax or configuration errors for the listed switch, the resulting configuration being pushed to the switch will be displayed in the right side of the popup. If there are any syntax errors in the template, or Central is otherwise unable to apply the configuration to the switch, this will be displayed instead.

Select **Close** to return to the **Configuration Audit** page.



The lower portion of the page provides access to the configuration backup and restore feature, and a list of devices in the group with **Config Sync** and **Template Error** status. Switches with no configuration or template issues are displayed with grey icons, while those with errors instead display a **red** icon.



Troubleshooting switch connectivity to Central

If a managed switch loses connectivity to Central, it will be displayed as Offline in the global or group device list under the Switches tab. The status of the connection to Activate and Central can be checked from the switch console using the `show aruba-central` CLI command.

```
switch# show aruba-central
Central admin state                : enabled

Central location                   : N/A
VRF for connection                 : N/A
Central connection status          : N/A

Central source                     : activate
Central source connection status    : N/A
Central source last connected on    : N/A
System time synchronized from Activate : False

Activate Server URL                 : devices-v2.arubanetworks.com
CLI location                        : N/A
CLI VRF                             : N/A

Source IP                          : N/A
Source IP Overridden                : False

Central support mode                : disabled
```

Check and correct the following when troubleshooting Central connectivity issues:

- Central admin state is **enabled**
- DNS resolution of Activate and Central hostnames (e.g. devices-v2.arubanetworks.com)
- Reachability of Activate and Central hosts from the switch on TCP port 443 (TLS/SSL)
 - Firewall rules may be required to permit outbound connections on TCP port 443
- HTTP proxy is configured on the VRF used for Central management, where required
- If Central location is provided by ZTP DHCP option or CLI override, ensure the correct FQDN or IPv4 address is defined for the Central instance managing the switch

Note that certain configuration changes pushed by Central, such as interface or DNS server configuration, may cause a temporary or persistent loss of connectivity when applied to the running configuration on the switch; ensure that proposed

configuration changes will not remove or change settings that are required to maintain or re-establish the management connection before applying them.

Applicable platforms

The content of the Aruba CX Hardening Guide is applicable to the following platforms:

- Aruba CX 6100 Switch Series
- Aruba CX 6200 Switch Series
- Aruba CX 6300 Switch Series
- Aruba CX 6400 Switch Series
- Aruba CX 8320 Switch Series
- Aruba CX 8325 Switch Series
- Aruba CX 8360 Switch Series
- Aruba CX 8400 Switch Series